@mindefarg
argentina.gob.ar/defensa
Ministerio de Defensa
Argentina
Edificio Libertador
Azopardo 250 (CABA)
(54 11) 4346-8836/9

Subsecretaría de Ciberdefensa

Boletín de Noticias de Ciberseguridad

Informe sobre incidentes y ciberamenazas Nro. 194 – Año 2022

Este boletín periódico es un resumen seleccionado de las últimas vulnerabilidades, incidentes de seguridad e informes recopilados de fuentes internacionales conocidas dedicadas a la seguridad informática. Está destinado a las áreas de ciberseguridad de la Defensa como información de interés general para su difusión.

Noticias de ciberseguridad entre el 25/11/22 y el 1/12/22

- Nuevos ataques de ransomware en Ucrania vinculados a los hackers rusos Sandworm.
  https://www.bleepingcomputer.com/news/security/new-ransomware-attacks-in-ukraine-linked-to-russian-sandworm-hackers/
- Una banda de ransomware intenta atacar a una municipalidad belga, pero en su lugar afecta a la policía.
  https://www.bleepingcomputer.com/news/security/ransomware-gang-targets-belgian-municipality-hits-police-instead/
- El ataque del ransomware Keralty afecta al sistema de salud de Colombia.
  https://www.bleepingcomputer.com/news/security/keralty-ransomware-attack-impacts-colombias-health-care-system/?utm_source=dlvr.it&utm_medium=twitter

TRABAJOS, ESTUDIOS Y ANÁLISIS ABOCADOS A LAS TEMÁTICAS DE LA CIBERSEGURIDAD

- **Informe: quiénes rastrearon a los usuarios de Internet en 2021-2022.**
  https://securelist.com/tracker-report-2021-2022/108079/
- Reporte especial: contraseñas más seguras.
  https://nordpass.com/es/most-common-passwords-list/
- Los documentos con texto protegido no son tan seguros como se cree.
  https://www.wired.com/story/redact-pdf-online-privacy/
- **Deloitte revela 10 predicciones estratégicas de ciberseguridad para 2023.**
  https://venturebeat.com/security/deloitte-cybersecurity-predictions-2023/
- **Detección de ransomware con la plataforma Wazuh SIEM y XDR.**
  https://www.bleepingcomputer.com/news/security/ransomware-detection-with-wazuh-siem-and-xdr-platform/
- Cloudflare encuentra un camino a través de las defensas de la red de China.
  https://www.theregister.com/2022/11/30/cloudflare_china_networking/
  https://blog.cloudflare.com/cloudflare-one-in-china/
- El ransomware Trigona ha sido identificado por el aumento de los ataques en todo el mundo.
  https://www.bleepingcomputer.com/news/security/trigona-ransomware-spotted-in-increasing-attacks-worldwide/
- Nuevo malware para Windows además roba datos de los teléfonos móviles de las víctimas.
  https://www.bleepingcomputer.com/news/security/new-windows-malware-also-steals-data-from-victims-mobile-phones/

NOTAS DE INTERÉS

- Los repositorios de Docker Hub esconden más de 1.650 contenedores maliciosos.
  https://www.bleepingcomputer.com/news/security/docker-hub-repositories-hide-over-1-650-malicious-containers/

- **Investigan la filtración de datos de WhatsApp: 500 millones de registros de usuarios en venta.**
https://securityaffairs.co/wordpress/138967/data-breach/whatsapp-data-leak-500m.html
- Se encuentra una vulnerabilidad de ejecución remota de código en Windows Internet Key Exchange.
https://www.infosecurity-magazine.com/news/rce-vulnerability-in-windows-ike/
- Estados Unidos prohíbe los equipos de telecomunicaciones y las cámaras de vigilancia chinas por riesgo para la seguridad nacional.
https://thehackernews.com/2022/11/us-bans-chinese-telecom-equipment-and.html
- Detallan la vulnerabilidad de la AppSync en Amazon Web Services.
https://thehackernews.com/2022/11/researchers-detail-appsync-cross-tenant.html
- Los controladores de dominio de Windows Server pueden detenerse y reiniciarse después de actualizaciones recientes.
https://www.theregister.com/2022/11/28/microsoft_windows_server_lsass/
- **Un error en algunas laptops de Acer puede utilizarse para eludir las funciones de seguridad.**
https://securityaffairs.co/wordpress/139055/hacking/acer-flaw-uefi-secure-boot.html
- CISA advierte de una vulnerabilidad crítica de Oracle Fusion Middleware.
https://thehackernews.com/2022/11/cisa-warns-of-actively-exploited.html
- La plataforma de formación cibernética del ejército de EE.UU., de Lockheed Martin, pasa a responder también al ámbito civil.
https://www.theregister.com/2022/11/29/lockheed_martin_cyber_training/
- **Los actores de la amenaza están ofreciendo acceso a las redes corporativas a través del ingreso no autorizado a la VPN de Fortinet.**
https://securityaffairs.co/wordpress/139085/cyber-crime/iabs-offers-access-via-fortinet-products.html
- Ciberespías chinos (UNC4191) utilizan dispositivos USB para atacar a entidades en Filipinas.
https://thehackernews.com/2022/11/chinese-cyber-espionage-hackers-using.html
- Nuevos errores en "Icefall" incluyen un fallo crítico de denegación de servicio. Afectan a millones de dispositivos OT.
https://www.infosecurity-magazine.com/news/new-icefall-bugs-include-critical/
- **Google revela los vínculos de una empresa informática española con el software espía centrado en Chrome, Firefox y Microsoft Defender.**
- https://www.cyberscoop.com/google-spyware-chrome-firefox-microsoft/
- La mayoría de los contratistas de defensa de EE.UU. no cumplen los requisitos básicos de ciberseguridad.
https://www.infosecurity-magazine.com/news/us-defense-contractors/
- Los legisladores de San Francisco aprueban los robots letales, pero no pueden llevar armas.
https://www.theregister.com/2022/11/30/san_francisco_killer_robots_ordinance/
- LastPass informa de otra filtración de datos de clientes.
https://www.infosecurity-magazine.com/news/lastpass-reveals-another-customer/

ACTUALIZACIONES DE SEGURIDAD

- Google publica actualización de emergencia de Chrome para corregir el octavo día cero de 2022.
https://www.zdnet.com/article/google-rushes-out-chrome-browser-fix-for-new-zero-day-flaw/
- NVIDIA publica una actualización del controlador de la GPU para corregir 29 fallos de seguridad.
https://www.bleepingcomputer.com/news/security/nvidia-releases-gpu-driver-update-to-fix-29-security-flaws/